

**BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND**



AIR FORCE INSTRUCTION 31-203

AIR FORCE MATERIEL COMMAND

Supplement 1

18 MAY 2005

Security

**SECURITY FORCES MANAGEMENT
INFORMATION SYSTEM (SFMIS)**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFMC WWW site at:

<https://www.afmc-mil.wpafb.af.mil/pdl/>

OPR: HQ AFMC/MSFOI (SMSgt Joe St. Cyr)

Certified by: HQ AFMC/MSFOI
(Lt Col Christine H. Ashenfelter)

Pages: 3

Distribution: F

AFI 31-203, 15 Aug 2001, is supplemented as follows:

This publication supplements AFI 31-203, *Security Forces Management Information System*, and provides additional and command-unique requirements. This supplement applies to all security forces organizations and personnel assigned to Air Force Materiel Command (AFMC) and aligns AFMC policy with the Air Force instruction.

1.2.5. At a minimum, each installation will conduct a monthly review of all reports containing Defense Incident-Based Reporting System (DIBRS) and National Incident-Based Reporting System (NIBRS) to ensure proper compliance. Errors should be corrected as soon as possible. The System Administrator (SA) must forward all issues to the SFMIS Field Assistance Branch (FAB), with concurrent notification to HQ AFMC/MSFOI, if errors cannot be corrected immediately.

1.2.6.1. The Security Forces Operations Branch (HQ AFMC/MSFOI) is responsible for policy, resource advocacy and oversight of this program for Air Force Materiel Command. All SFMIS users are required to complete web-based training. The SFMIS administrator must forward a signed letter or e-mail to HQ AFMC/MSFOI on each individual within 30 days of gaining access to SFMIS. HQ AFMC/MSFOI will distribute training from the FAB when available, but is not sufficient to train all individuals requiring access. CSFs will establish unit training requirements for SFMIS users. Systems Administrators are required to document the training in the individual's training records and to have the training records available in the work centers.

1.2.7.1. CSF will appoint a primary and alternate SA in writing and forward a copy to HQ AFMC/MSFOI (electronically signed e-mails are acceptable.) The SA at each installation will also serve as the single focal point for all installation SFMIS issues. Units are responsible for maintaining a current list of SFMIS users and the modules to which they are authorized. This list must be forwarded annually to HQ AFMC/MSFOI NLT 1 January or as changes occur.

1.2.7.2. As a minimum, the SA will develop instructions that include guidelines and procedures for proper implementation, management, training and access control of the SFMIS program. The overall objective is to ensure integrity of the system and protection of personal data information.

1.2.7.5. (Added) Any questions or problems regarding SFMIS modules should be addressed to the FAB and sent to HQ AFMC/MSFOI for inclusion with command correspondence to AFSFC and the FAB. SAs will forward concerns and inputs to HQ AFMC/MSFOI for inclusion in command communications with the AFSFC and FAB offices. Day-to-day questions or issues may be addressed directly to the FAB for timely resolution.

3.2. Hardware/Software Requirements. Units will consider SFMIS requirements when replacing computers within the unit. CSFs should establish procedures to ensure future expenses for modernization of the system are reflected in the annual budgets.

3.2.3. As technology advances, the CSF and the SA will comply with minimum SFMIS system hardware and software standards. SF squadrons will also develop a SFMIS life-cycle-system plan and annual budget to accommodate future upgrades and enhancements.

3.2.4. Units will use all modules and are required to develop a plan to fully integrate these modules into daily operations. **EXCEPTION:** The issue and turn-in function is not required to be integrated until units receive card readers and scanners to expedite issue and turn-in.

3.2.4.1. (Added) All deviations to the use of SFMIS must be submitted in memorandum format through HQ AFMC/MSF, who will in turn coordinate them with AFSFC for final approval.

3.2.4.2. (Added) Utilization of Commercial-Off-The-Shelf (COTS) information management systems are not authorized without HQ AFMC/MSF approval. Units will coordinate all issues involving procurement of any COTS information management systems with HQ AFMC/MSF prior to purchase of COTS software and hardware. The requirements in AFI 31-101 for production of automated entry card systems are applicable and MAJCOM approval will be coordinated prior to purchase and implementation.

3.3.2. Squadron SAs must develop lockout procedures and necessary actions to assign new passwords for all SFMIS users.

3.3.3. Squadron SAs will monitor, manage and develop procedures to immediately report known violations of the system operation or unauthorized dissemination of "For Official Use Only" (FOUO) information. Completed reports will be forwarded by the violator's unit commander to HQ AFMC/MSFOI no later than 15 duty days from the date of occurrence.

3.3.4. Squadron SAs will be the focal point in coordinating with all base functions that may require access to SFMIS information.

4.3.1. (Added) Maintain an SFMIS continuity book, to include a log of all trouble tickets established with the FAB. Establish a log each calendar year and maintain it for 1 year.

4.3.2. (Added) If adequate assistance is not provided in a timely manner, submit a written report (email permitted) to HQ AFMC/MSFOI explaining the service problems with the FAB.

CHERYL L. DOZIER, Colonel, USAF
Chief of Security Forces
Directorate of Mission Support